

What is claimed is:

1. A transmission apparatus comprising:
encryption means for encrypting data and producing first encrypted data;
5 program-specific information generating means for producing program-specific information containing a table denoting the correlation between first encrypted data and a program number of the first encrypted data;
tool list generating means for producing a tool list containing a tool ID indicating a decoding tool for decrypting the first encrypted data;
10 control graph generating means for producing a control graph indicating the instantiated location of the decoding tool in the receiving apparatus;
rights information generating means for producing rights information for the first encrypted data; and
multiplexing means for multiplexing the first encrypted data, program-
15 specific information, tool list, control graph, and rights information.

2. A transmission apparatus comprising:
encryption means for encrypting data and producing first encrypted data;
20 tool list generating means for producing a tool list containing a tool ID indicating a decoding tool for decrypting the first encrypted data;
control graph generating means for producing a control graph indicating the instantiated location of the decoding tool in the receiving apparatus;
rights information generating means for producing rights information
25 for the first encrypted data; and
program-specific information generating means for producing

program-specific information containing a table denoting the correlation between first encrypted data and a program number of the first encrypted data, the tool list, the control graph, and the rights information; and

5. multiplexing means for multiplexing the first encrypted data and the program-specific information.

3. A transmission apparatus comprising:

encryption means for encrypting data and producing first encrypted data;

10 tool list generating means for producing a tool list containing a tool ID indicating a decoding tool for decrypting the first encrypted data;

control graph generating means for producing a control graph indicating the instantiated location of the decoding tool in the receiving apparatus;

15 program-specific information generating means for producing program-specific information containing a table denoting the correlation between first encrypted data and a program number of the first encrypted data, the tool list, the control graph, and the rights information; and

rights information generating means for producing rights information for this data;

20 rights information transmission means for outputting the rights information; and

multiplexing means for multiplexing and outputting the first encrypted data and the program-specific information.

25 4. A transmission apparatus as described in claim 3, wherein the rights information transmission means relates the rights information to the data.

5. A transmission apparatus as described in claim 3, wherein the program-specific information generating means relates the rights information to the data.

5

6. A transmission apparatus as described in claim any of claims 1 to 5, wherein the multiplexing means multiplexes the decoding tool used for decryption.

7. A transmission apparatus as described in claim any of claims 1 to 6, 10 wherein the multiplexing means multiplexes key information enabling decryption.

8. A receiving apparatus comprising:
15 demultiplexing means for separating a multiplexed signal containing first encrypted data into at least the first encrypted data and program-specific information;

20 tool list demultiplexing means for separating a tool list having a tool ID indicating a decoding tool for decrypting the first encrypted data from the multiplexed signal;

control graph demultiplexing means for separating a control graph 25 indicating the instantiated location of the decoding tool in the receiving apparatus from the multiplexed signal;

rights information demultiplexing means for demultiplexing rights information for the first encrypted data from the multiplexed signal;

25 first control means for acquiring a tool according to a tool ID acquired from the tool list, and instantiating the tool according to the control graph; and

first rights management means for processing the first encrypted data

according to the rights information.

9. A receiving apparatus comprising:
demultiplexing means for separating a multiplexed signal containing
5 first encrypted data into at least the first encrypted data and program-specific
information;
tool list demultiplexing means for separating a tool list having a tool ID
indicating a decoding tool for decrypting the first encrypted data from the
multiplexed signal;
10. control graph demultiplexing means for separating a control graph
indicating the instantiated location of the decoding tool in the receiving apparatus
from the program-specific information;
- 15 rights information demultiplexing means for demultiplexing rights
information for the first encrypted data from the program-specific information;
- 15 first control means for instantiating a tool with a tool ID acquired from
the tool list according to the control graph; and
first rights management means for processing the first encrypted data
according to the rights information.

- 20 10. A receiving apparatus comprising:
demultiplexing means for separating a multiplexed signal containing
first encrypted data into at least the first encrypted data and program-specific
information;
tool list demultiplexing means for separating a tool list having a tool ID
25 indicating a decoding tool for decrypting the first encrypted data from the
multiplexed signal;

control graph demultiplexing means for separating a control graph indicating the instantiated location of the decoding tool in the receiving apparatus from the program-specific information;

first control means for instantiating a tool with a tool ID acquired from

5 the tool list according to the control graph;

rights information receiving means for receiving rights information for the first encrypted data; and

first rights management means for processing the first encrypted data according to the rights information.

10

11. A receiving apparatus as described in any of claims 8 to 10, further comprising:

temporary storage means for temporarily storing the received first encrypted data; and

15 reading means for reading the first encrypted data stored to the temporary storage means.

12. A receiving apparatus as described in claim 11, further comprising file management means for deleting from the temporary storage means the first encrypted data after the playback permit recorded in the rights information is 20 expired.

13. A receiving apparatus as described in any of claims 8 to 12, wherein the rights management means sends status information denoting the processing 25 state of the first encrypted data.

14. A receiving apparatus as described in any of claims 8 to 13, further comprising:

rights management means for separating the rights information into first rights information and second rights information;

5 multiplexing adjusting means for rewriting rights information in the multiplexed signal to second rights information, and outputting a revised multiplexed signal;

wherein the revised multiplexed signal is output to a second receiving apparatus according to a request signal from the second receiving apparatus.

10

15. A receiving apparatus as described in any of claims 8 to 13, further comprising:

rights management means for separating the rights information into first rights information and second rights information;

15

wherein the second rights information and multiplexed signal are output to a second receiving apparatus according to a request signal from the second receiving apparatus.

16. A receiving apparatus as described in any of claims 8 to 15, wherein

20 the rights management means receives data indicating how the first encrypted data was processed by a second receiving apparatus, and sends status information describing processing by said receiving apparatus and the second receiving apparatus.

25 17. A receiving apparatus as described in any of claims 8 to 16, further comprising:

conversion means for converting the first encrypted data to second encrypted data; and

remultiplexing means for remultiplexing the second encrypted data with the second rights information.

5

18. A receiving apparatus as described in any of claims 8 to 17, wherein the first encrypted data is processed according to the first rights information.

19. A receiving apparatus as described in any of claims 8 to 18, further 10 comprising:

file management means for deleting the first encrypted data from the temporary storage means after sending it to a second receiving apparatus.

20. A receiving apparatus as described in any of claims 8 to 19, further 15 comprising:

video decoding means for extracting and decoding video data from the multiplexed signal.

21. A receiving apparatus as described in any of claims 8 to 19, further 20 comprising:

audio decoding means for extracting and decoding audio data from the multiplexed signal.